

FILED

MAR - 7 2024

CLERK, U.S. DISTRICT COURT

By _____ Deputy

Case No. 4:24-MJ-179

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
)
 Target Devices 1-3, seized from Charles Lloyd BRITT,
 Jr. and presently secured at the HSI Dallas Field Office
)

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Target Devices 1-3, seized from Charles Lloyd BRITT, Jr. and presently secured at the HSI Dallas Field Office, as further described in Attachment A.

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2251, 2252, 2252A, and 2422	Sexual exploitation of children, receipt and possession of child pornography, and coercion and enticement

The application is based on these facts:

See attached Affidavit of HSI Special Agent Tyler Booth.

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Tyler Booth, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 3/7/2024

City and state: Fort Worth, Texas



Judge's signature

United States Magistrate Judge Hal R. Ray, Jr.

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Tyler Booth, being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since June 2019. I am a graduate of the Criminal Investigator Training Program and HSI Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code. I am an “investigative or law enforcement officer of the United States” within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to the sexual exploitation of children, including the illegal coercion and enticement of minors, and the production, distribution, receipt, transportation, and possession of child pornography, in violation of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A. I have received training in the area of child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in numerous child pornography investigations, and I am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is being made in support of an application for a warrant authorizing the search of an Acer One 14 laptop computer, displaying serial number NXG80SP01253404C0B4P00, a black Apple iPhone cellular phone, and a black Samsung Android cellular phone bearing IMEI# 355181115320706 (hereinafter, “**TARGET**”

DEVICES"), seized from Charles Lloyd BRITT Jr. The TARGET DEVICES are presently secured at the HSI Dallas Field Office in Irving, Texas, which is within the Northern District of Texas. I seek authorization to search this device for items specified in Attachment B incorporated with this affidavit, which constitute evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 (production, receipt and possession of child pornography and enticement of a minor).

4. The information set forth in this affidavit comes from an investigation I have conducted, my training and experience, and information provided to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422, or the attempt to commit such violations, are presently located within the **TARGET DEVICES**.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is an Acer One 14 laptop computer, displaying serial number NXG80SP01253404C0B4P00, a black Apple iPhone cellular phone, and a black Samsung Android cellular phone bearing IMEI# 355181115320706 (hereinafter, "**TARGET DEVICES**"). These **TARGET DEVICES** were seized at DFW airport from the custody of Charles Lloyd BRITT Jr. and are presently secured at the HSI Dallas Field Office in Irving, Texas, which is within the Northern District of Texas.

6. The applied-for warrant would authorize the continued seizure and the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

DEFINITIONS

7. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and Attachment B:

- a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Computer" refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, "computer" also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. *See* 18 U.S.C. § 1030(e)(1).
- c. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, external storage devices, floppy

disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the provider assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

e. “Mobile applications” or “mobile apps” are computer programs or software applications specifically designed to run on mobile electronic devices (e.g., smartphones, tablets, e-readers, etc.). Mobile applications are generally downloaded from application distribution platforms operated by specific mobile operating systems, like App Store(Apple mobile devices) or Google Play Store (Android mobile devices).

f. “Instant messaging” is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating and gaming websites and mobile applications offer instant messaging for users to communicate amongst themselves.

More advanced features of instant messaging include push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

g. A “hash value” is value given to a file or data after a mathematical function converts the data into an alpha-numeric value. A hash value is akin to a digital fingerprint, in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. A hash value is unique to the specific data from which the hash value was generated. Hash values can be used to search for identical data stored on various digital devices, as identical data will have the same hash value.

h. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, flash drives, digital video disks or DVD’s, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my training and experience in child exploitation investigations, I am aware that computers, computer technology, and the Internet significantly facilitate the production, receipt, distribution, and possession of child pornography, as well as the transportation of minors. Computers generally serve five (5) functions in connection with child exploitation offenses: production, communication, distribution, storage and social networking. Child exploitation offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. A smartphone or other camera equipped mobile device (e.g. tablet) is capable of not only producing child pornography images directly with the device's camera, but of also transmitting child pornography images via the use of the Internet. Therefore, through use of the Internet, electronic contact can be made to literally millions of computers, smartphones, and other wireless electronic devices around the world.

9. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in personal computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as smartphones (e.g., Apple iPhones, Samsung Galaxy), connected devices (e.g., Apple iTouch), e-readers, and tablets (e.g., Apple iPads, Kindle Fire) now function essentially as computers with the same abilities to store images in digital form.

10. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive in space that is not allocated to an active file for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

11. Additionally, a computer user's Internet activity generally leaves traces in a computer's web cache and Internet history files. Files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically maintain a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each of the Devices was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

OVERVIEW OF INVESTIGATION

13. On March 1, 2024, Customs and Border Protections (CBP) Officers called HSI Dallas about a subject identified as Charles Lloyd BRITT Jr. possibly being in possession of sexually explicit videos of children. The CBP Officers stated BRITT was a United States citizen traveling from Doha, Qatar to DFW Airport on Qatar Airlines flight 731. Pursuant to border search authority, when BRITT arrived at the Dallas-Fort Worth International Airport, CBP Officers encountered BRITT and reviewed his cellular phone, which appeared to contain videos of minor females engaged in sexually explicit conduct. After CBP requested assistance from HSI, I responded to CBP and confirmed the videos discovered on BRITT's black Samsung Android cellular phone, bearing IMEI# 355181115320706, depicted minor females involved in sexually explicit conduct. I observed multiple videos depicting prepubescent minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(8)(A), including one video which depicted a prepubescent minor female involved in sexual intercourse with two adult males.

14. I interviewed BRITT after reading him his *Miranda* warnings, and he admitted that he knew the videos were on his phone. BRITT also stated that he started looking at child pornography years ago and that he was sure that forensic analysts would find searches for child pornography on his devices. BRITT later denied that child pornography would be found on his laptop, but then stated it was possible that it would contain child pornography. BRITT also said that he received messages and videos of child pornography through WhatsApp, though he deleted the messages and kept the videos. Finally, BRITT acknowledged that he had had a Skype conversation in 2018 that involved seeing a 10-year-old boy. He also acknowledged sending money to women in the Philippines who have shown him child pornography or show him nude kids in a format that I believe is live-streaming.

15. During the inspection of BRITT, CBP officers also located a black Apple iPhone cellular phone, and an Acer One 14 laptop computer, displaying serial number NXG80SP01253404C0B4P00. These devices, along with the black Samsung Android cellular phone, were seized by HSI.

16. Based on my training and experience, individuals who download and view images and videos of child pornography will often use multiple devices to conduct this activity. I also know that individuals frequently back up their cellular phone content to their computers. Therefore, I seek authorization from this Court to continue to seize these devices and to search all the **TARGET DEVICES** and all of its contents, including any synchronized applications or incorporated data cards, to seize the items specified in Attachment B, which constitute evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.

**SPECIFICS REGARDING THE SEARCH AND SEIZURE OF
SMARTPHONES AND MOBILE ELECTRONIC DEVICES**

17. Smart cellular telephones (smartphones), in addition to functioning as a handheld wireless electronic communication device capable of making and receiving telephone calls, can function as a video camera, a camera phone, a portable media player, and an Internet client with email and web browsing capabilities with Wi-Fi and cellular data connectivity. In addition to all of the above capabilities, smartphones also provide basic functions such as, but not limited to: (1) storing names and phone numbers in electronic "address books;" (2) sending, receiving, and storing text messages and email; (3) taking, sending, receiving, and storing still photographs and moving video; (4) storing and playing back audio files; (5) storing dates, appointments, and other information on personal calendars; (6) accessing and downloading information from the Internet; and (7) receiving, accessing, and storing voice mail. In addition, smartphones are capable of running applications such as Google Hangouts, Google Maps, and hotel booking applications.

18. Smartphones are also designed to connect to personal computers to share files, share internet connections, perform backup functions, and charge the phone battery. Smartphone users commonly synchronize their data files, including image files, to personal computers to maintain a backup of these files.

19. Based on my training and experience, I am aware smartphones and other mobile electronic devices (e.g., tablets, e-readers, etc.) are fundamentally computers under 18 U.S.C. § 1030(e)(1), and are generally capable of acting as electronic storage devices.

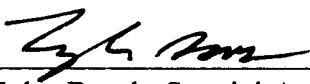
Furthermore, they are capable of connecting to computer networks, including the Internet, via cellular radio and/or Wi-Fi. I know, based on my training and experience, modern cellular telephones are essentially computers with a smaller, pocket-sized footprint. They have advanced processors, high-definition displays, and mass data storage. High-end cellular phones can be equipped with up to 1 TB of data storage. As small computers, cellular telephones must be searched in a similar way to computers. Moreover, due to their portability, file system design, and mass data storage, files may be stored anywhere on the device. In my training and experience, users who produce, possess, transport, receive or otherwise traffic in child pornography will often hide files in unsuspecting locations on a cellular telephone to avoid detection by others. I have observed individuals using special applications designed specifically to encrypt and/or conceal their contents for the purpose of hiding child pornography from law enforcement. Due to these factors, it is necessary to search the entire contents of a cellular telephone for evidence of child pornography. I seek authorization from this Court to search the **TARGET DEVICES** and all of its contents, including any synchronized applications or incorporated data cards, to seize the items specified in Attachment B, which constitute evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2422(b) and 2423.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, which might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

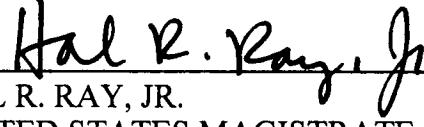
CONCLUSION

22. Based on the information set forth in this affidavit, including the discovery of child pornography on BRITT's Samsung cellular phone and his statements about other child exploitative conduct, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 are presently located within all of the **TARGET DEVICES**, more specifically described in Attachment A. Accordingly, I respectfully request that this Court authorize the search of these devices, so that the government may search for and seize the items listed in Attachment B.



Tyler Booth, Special Agent
Homeland Security Investigations

Sworn to before me and subscribed in my presence this 7TH day of March 2024, at
11:07 a.m. in Fort Worth, Texas.

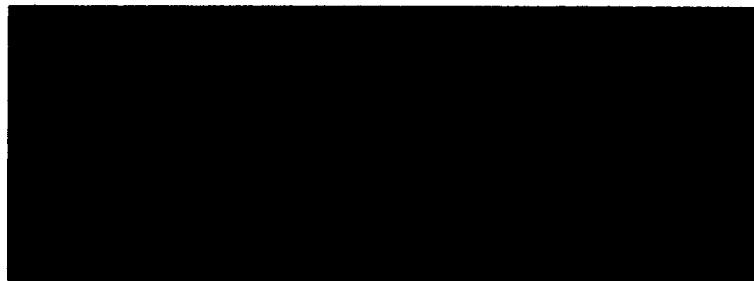


HAL R. RAY, JR.
UNITED STATES MAGISTRATE JUDGE

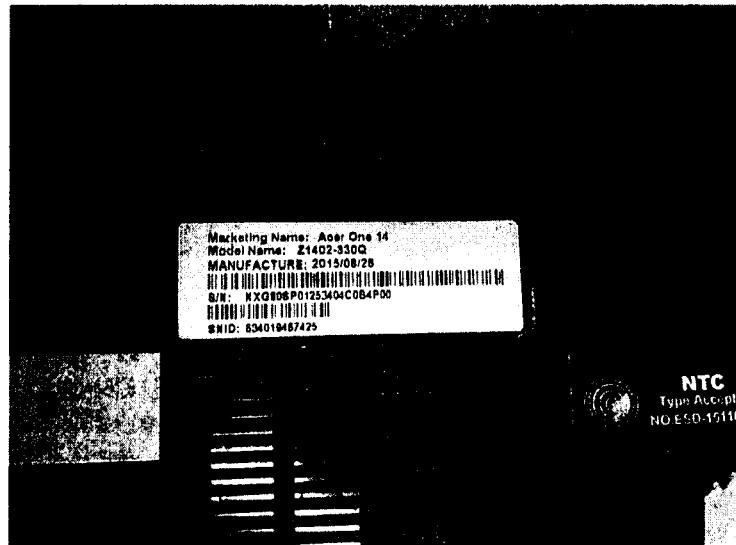
ATTACHMENT A
DESCRIPTION OF ITEM TO BE SEARCHED

The devices were seized at DFW airport from the custody of Charles Lloyd BRITT Jr. and are presently secured at the HSI Dallas Field Office, 125 E. John Carpenter Freeway Suite 800, Irving, Texas, which is located within the Northern District of Texas. The items to be searched are described as follows:

A Black, Samsung Android cellular phone bearing IMEI# 355181115320706



An Acer One 14 laptop computer, displaying serial number NXG80SP01253404C0B4P00



A Black, Apple iPhone Cellular Telephone



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

Contraband, evidence, fruits and instrumentalities of the coercion and enticement of minors, and the production, transportation, distribution, receipt or possession of child pornography as defined in 18 U.S.C. § 2256(8), in any form, including, but not limited to:

1. Electronic devices, including computer(s), mobile/smart phones, computer hardware, computer software, computer related documentation, computer passwords and data security devices that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Videos, still images, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. Written, typed, or verbal communications between Charles Lloyd BRITT Jr. and other individuals, which may constitute violations of 18 U.S.C. §§ 2251, 2252, 2252A and 2422;
4. Evidence of smartphone applications or other programs used to receive, transport, and possess child pornography as well as to solicit or entice minors to engage in sexually explicit conduct, or to produce images of minors engaged in sexually explicit conduct;
5. Evidence of who used, owned, or controlled the device at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence; evidence of the times the devices were used;

6. Passwords, encryption keys, and other access devices that may be necessary to access the devices, applications on the devices, or remote storage services;
7. Records of or information about Internet Protocol addresses used by the device;
8. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
9. Credit card information including but not limited to bills and payment records related to the use of mobile applications and remote storage;
10. Information or correspondence pertaining to affiliation with any child exploitation websites or social media applications;
11. Any material that is "child erotica," including clothed images of minors with whom Charles Lloyd BRITT Jr. engaged in sexually explicit communications;
12. Any images, videos, correspondence, or other files reflecting any relationship between Charles Lloyd BRITT Jr. and any minor.